Distr.: Limited
4 April 2018

English only

Expert Group to Conduct a Comprehensive Study on Cybercrime
Vienna, 3-5 April 2018

Draft report

Addendum

II. Recommendations (*continued*)

Criminalization (item 3)

1. In line with the Chair's proposal for the 2018–2021 workplan of the Expert Group, adopted by the meeting on its 1st day, at the meetings of the Expert Group in 2018, 2019 and 2020, the Rapporteur, with the necessary assistance of the Secretariat and based on the discussions and deliberations, will prepare a list of preliminary conclusions and recommendations suggested by Member States, which should be precise and focus on strengthening practical responses to cybercrime. Also according to the workplan, the list will be included in the summary report of the meeting as a compilation of suggestions made by Member States, for further discussion at the stocktaking meeting in 2021. The workplan also states that the Expert Group stocktaking meeting will finish consideration of all the preliminary conclusions and recommendations and will produce a consolidated list of adopted conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice.

2. Accordingly, the following is the compilation of suggestions made by Member States at the fourth session of the Expert Group in relation to agenda item 3 "Criminalization":

(a) Member States should take into account that many substantive criminal law provisions for offline crime can also be applicable for crimes committed online and therefore they should use, for the purpose of strengthening law enforcement, existing provisions in domestic and international law, where appropriate, to tackle those crimes in the online environment;

(b) Member States should adopt and apply domestic legislation to criminalize cybercrime conduct and to provide procedural legal authority to permit law enforcement authorities to investigate alleged crimes consistent with due process guarantees, privacy interests, civil liberties and human rights;

(c) Member States should further pass cyber-specific criminal legislation which takes into account new criminal conduct associated with the misuse of ICTs to avoid relying on generally applicable criminal laws;

Please recycle

(d) Member States should criminalize, taking into account widely recognized international standards, core cybercrime offences that affect the confidentiality, integrity and availability of computer networks and computer data;

(e) Cyber-related acts that are minor infringements rather than of a criminal nature should be addressed by civil and administrative regulations as opposed to criminal legislation;

(f) Member States should consider, if they have not done so, the criminalization of:

- New and emerging forms of cybercrime activities such as the criminal misuse of cryptocurrencies, offences committed on the darknet, the Internet of things, phishing, distribution malwares, and any other software for criminal acts;
- The disclosure of personal information so called "revenge porn";
- The use of Internet for the purpose of terrorism;
- The use of Internet to incite hate crime and violent extremism;
- The provision of technical support or assistance for the perpetration of cybercrime;
- The establishment of illicit online platforms or publishing information for the purpose of perpetrating cyber-related crimes;
- Illegally accessing or hacking into computer systems;
- Illegal interception of, or damage to, computer systems or data;
- Illegal data and system interference;
- Misuse of devices;
- Computer related forgery and fraud;
- Child sexual abuse and exploitation;
- The infringement of copyrights.

(g) Member States should bear in mind that the focus of international harmonization concerning criminalization of cybercrime should be on a core set of offences against the confidentiality, integrity and accessibility of information systems, while a need to harmonize criminalization concerning general offences that are committed using information and communication technology should mainly be dealt with in specialized forums concerning specific areas of crime;

(h) Member States should avoid criminalizing a broad range of activities by Internet service providers, especially where such regulations may improperly limit legitimate speech and expression of ideas and beliefs. Member States should instead work with Internet service providers and the private sector to strengthen cooperation with law enforcement authorities, noting in particular that most Internet service providers have a vested interest in ensuring that their platforms are not abused by criminal actors;

(i) Member States should adopt and implement a domestic legal evidence framework to permit the admission of electronic evidence in criminal investigations and prosecutions, including appropriate sharing of electronic evidence with foreign law enforcement partners;

(j) Member States should use the United Nations Convention against Transnational Organized Crime (UNTOC) to facilitate information and evidence sharing for such criminal investigations, given the frequent involvement of organized crime groups in cybercrime;

(k) Member States should explore ways to help ensure that the exchange of information among investigators and prosecutors dealing with cybercrime is made in

a timely and secure way, including by strengthening networks of national institutions that may be available 24/7;

(l) On the issue of criminalizing ISP's non-compliance with law enforcement, Member States should pay meticulous caution to the detrimental effects on private sector activities and fundamental human rights, in particular, freedom of speech;

(m) In addressing effectively cybercrime, Member States should take into consideration existing human rights frameworks, in particular as regards freedom of expression and the right to privacy; and should further uphold the principles of legality, necessity and proportionality, in criminal proceedings relating to the fight against cybercrime;

(n) Member States should identify trends in the underlying activities of cybercrime through research and further evaluate the possibility and feasibility of mandating the Expert Group or UNODC to conduct and make available on an annual basis, with substantive contributions by Member States, an assessment of cybercrime trends;

(o) Member States should consider the adoption of comprehensive strategies against cybercrime, aimed at developing victimization surveys as well as informing and empowering potential victims of cybercrime. Member States should also consider taking further preventive measures against cybercrime including measures for the responsible use of Internet, especially by children and young people.

III. Summary of deliberations (*continued*)

C. Criminalization

3. At its 4th and 5th meetings, on 4 and 5 April 2018, the Expert Group considered agenda item, entitled "Criminalization".

4. The discussion was facilitated by the following panellists: Malini Govender (South Africa), Li Jingjing (China), Vadim Sushik (Russian Federation), Eric do Val Lacerda Sogocio (Brazil), Marouane Hejjouji (Morocco) and Norman Wong (Canada).

5. Many speakers provided information on the ways in which cybercrime was criminalized in their countries. The most common offences mentioned by speakers included cyber-specific offences, often referred to as "core" cybercrime offences, such as those targeting the confidentiality, integrity and accessibility of computer systems as well as cyber-enabled offences, including offences related to child abuse and exploitation, privacy-related offences, personal data-related offences, the use of the Internet for terrorist purposes, among others. Speakers noted that most countries have legislation already in place to criminalize the core cybercrime offences. It was noted by speakers that it was not necessary for States to have the same crime typology as long as the underlying conducts constituted offences in all jurisdictions, in order to comply with the principle of dual criminality and to eliminate safe havens for criminals.

6. Speakers also emphasized that legislation on the admission of electronic evidence in criminal investigations and prosecutions was needed in order to effectively counter cybercrime, which should be accompanied by adequate training and capacity-building for law enforcement, prosecutors and judges. The importance of sharing of electronic evidence among jurisdictions was also underscored.

7. Speakers shared the experience of their countries in devising legislation and laws to criminalize cybercrime activities. In this regard, experts shared when it was necessary to create new, specific legislation to criminalize certain acts, and when previously-existing legislation and general offences were adequate and sufficient to criminalize new and emerging forms of cybercrime. Many speakers expressed that it was very useful for legislation to be technology-neutral in order to remain applicable in the face of evolving forms of ICTs and cybercrime. It was also noted that each

country had different needs and could consider whether they needed to create new offences depending on the crime trends they faced. Speakers also noted the necessity of having adequate legislation to criminalize new and emerging forms of crime, such as the criminal misuse of cryptocurrency, the internet of things and the dark net, among others.

8. It was also noted that, at the same time, it was important to take into account human rights safeguards when requiring compliance from Internet service providers (ISPs). The Expert Group also discussed types of sanctions for ISPs who failed to cooperate with law enforcement as well as the ways in which the private sector could cooperate in with law enforcement.

9. Regarding the prevention of cybercrime, several speakers emphasized the importance of developing awareness-raising campaigns for the general public as well as targeted education programmes for children in order to inform them about the risks of cybercrime and to improve online safety and cybersecurity for the country as a whole. Moreover, it was stressed that tailored training courses and appropriate allocation of resources were needed in order to enhance the capacities of law enforcement to prevent cybercrime activities.

IV. Organization of the meeting

B. Statements (*continued*)

Criminalization (item 3)

10. Statements were made by experts of the following States: Guatemala, Japan, Colombia, Russian Federation, Norway, Canada, United States of America, India, China, Sri Lanka, Islamic Republic of Iran, Costa Rica, Norway, Indonesia, Philippines, Tunisia, Thailand, South Africa, Belarus, Algeria, Brazil, Ghana, Netherlands, Czechia, Ukraine, Germany, Romania, Lichtenstein, Moldova, Mexico, Serbia, Nigeria, Senegal, Japan, Georgia, Portugal.

11. Statements were also made by representatives of the following intergovernmental organizations: Council of Europe, European Union.